UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/634,507	08/05/2003	Osamu Kawamura	82478-0100	6906

21611 7590 05/16/2007

SNELL & WILMER LLP (OC)
600 ANTON BOULEVARD
SUITE 1400
COSTA MESA, CA 92626

EXAMINER	
GERGISO, TECHANE	
ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
05/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/634,507	KAWAMURA ET AL.	
	Examiner	Art Unit	
	Techane J. Gergiso 7-6	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1- 2 and 7-19* is/are rejected.

7)☒ Claim(s) *3-6* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is a final Office Action in response to the applicant's correspondence filed on February 28, 2007.

2. The applicant added new claims 13-19.

3. Claims 1-19 have been considered and are pending.

Response to Arguments

4. Applicant's arguments with respect to claims 1-19 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 2, 7 and 10-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Admitted prior art by applicant (hereinafter referred to as Admission) in view of Markham (US Pat. No.: 5, 796, 836).

As per claim 1:

Admission discloses a parallel stream operation apparatus, comprising:

an input stream processing unit receiving a plurality of data streams in parallel, and outputting each data stream to the one of the paths that corresponds to a key that, from among the plurality of keys, is for one of encrypting and decrypting the data stream (figure 1: 1621, 1601-1605; page 2: lines 6-19; page 3: lines 15-25); and

an operation unit performing, with respect to each of the data streams output to the paths, one of decryption and encryption using the key in correspondence with the path to which the data stream was output (figure 1: 1661; page 3: lines 19-25).

Admission discloses a different one of a plurality of keys used for encrypting and/or decrypting data streams (figure 1: 1631-1634). Admission does not explicitly disclose a plurality of paths; each corresponding to a different one of a plurality of keys used for one of encrypting and decrypting data streams. Markham, in analogous art, however, discloses a plurality of paths, each corresponding to a different one of a plurality of keys used for one of encrypting and decrypting data streams (figure 8a: 34; 92, 90, 88; column 13: lines 20-30; lines 55-64). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Admission to include a plurality of paths, each corresponding to a different one of a plurality of keys used for one of encrypting and decrypting data streams. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide system and method for decoupling encryption of one plain text block from the encryption of the next plain text block and encryption apparatus can be placed in parallel to increase throughput through the encryption circuit as suggested by Markham in (column 3: lines 35-40; column 4: lines 4-8).

As per claim 2:

Admission discloses a parallel stream operation apparatus, comprising:

an output stream processing unit receiving the plurality of data streams that have been decrypted or encrypted by the operation unit, and output each received data stream to a different one of a plurality of output interfaces (figure 1: 1661, 1681-1685).

As per claim 7:

Markham discloses a parallel stream operation apparatus, comprising:

a re-input path for re-inputting, into the input stream processing unit, one of the data streams that has already been encrypted or decrypted and output by the operation unit, wherein the operation unit encrypts or decrypts the input data stream that has already been encrypted or decrypted, using a key that is different to a key previously used to encrypt or decrypt the data (figure 11a: 52.1, 52.2. 52.3).

As per claim 10:

Admission discloses a parallel stream operation method used in a parallel stream operation apparatus that includes a plurality of paths, each of the paths corresponding to a different one of a plurality of keys used for one of encrypting and decrypting data streams, the method comprising:

an input stream processing step of receiving a plurality of data streams in parallel, and outputting each data stream to a the one of the paths that corresponds to a key that

from among the plurality of keys is for one of encrypting and decrypting the data stream (figure 1: 1621, 1601-1605; page 2: lines 6-19; page 3: lines 15-25); and

an operation step of with respect to each of the data streams output to the paths, performing one of decryption and encryption using the key in correspondence with the path to which the data stream was output (figure 1: 1661; page 3: lines 19-25).

As per claim 11:

Admission discloses a parallel stream operation program executed in a computer in a parallel stream operation apparatus that includes a plurality of paths, each of the paths corresponding to a different one of a plurality of keys used for one of encrypting and decrypting data streams, the program comprising:

an input stream processing step of receiving a plurality of data streams in parallel, and outputting each data stream to the one of the paths that corresponds to a key that from among the plurality of keys is for one of encrypting and decrypting the data stream (figure 1: 1621, 1601-1605; page 2: lines 6-19; page 3: lines 15-25).

an operation step of with respect to each of the data streams output to the paths, performing one of decryption and encryption using the key in correspondence with the path to which the data stream was output (figure 1: 1661; page 3: lines 19-25).

Admission discloses a different one of a plurality of keys used for encrypting and/or decrypting data streams (figure 1: 1631-1634). Admission does not explicitly disclose a plurality of paths, each corresponding to a different one of a plurality of keys used for one of encrypting and decrypting data streams. Markham, in analogous art, however, discloses a plurality of paths, each corresponding to a different one of a plurality of keys used for one of encrypting and decrypting data streams (figure 8a: 34; 92, 90, 88; column 13: lines 20-30; lines 55-64). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Admission to include a plurality of paths, each corresponding to a different one of a plurality of keys used for one of encrypting and decrypting data streams. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide system and method for decoupling encryption of one plain text block from the encryption of the next plain text block and encryption apparatus can be placed in parallel to increase throughput through the encryption circuit as suggested by Markham in (column 3: lines 35-40; column 4: lines 4-8).

As per claim 12:

Admission discloses a television reception apparatus, comprising:

an input stream processing unit sp receiving a plurality of data streams in parallel, and outputting each data stream to a the one of the paths that corresponds to a key that from among the plurality of keys is for one of encrypting and decrypting the data stream (figure 1: 1621, 1601-1605; page 2: lines 6-19; page 3: lines 15-25); and

an operation unit to performing, with respect to each of the data streams output to each of the paths one of decryption and encryption using the key in correspondence with the path to which the data stream was output an operation unit performing, with respect to each of the data streams output to the paths, one of decryption and encryption using the key in correspondence with the path to which the data stream was output (figure 1: 1661; page 3: lines 19-25).

Admission discloses a different one of a plurality of keys used for encrypting and/or decrypting data streams (figure 1: 1631-1634). Admission does not explicitly disclose a plurality of paths, each corresponding to a different one of a plurality of keys used for one of encrypting and decrypting data streams. Markham, in analogous art, however, discloses a plurality of paths, each corresponding to a different one of a plurality of keys used for one of encrypting and decrypting data streams (figure 8a: 34; 92, 90, 88; column 13: lines 20-30; lines 55-64). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Admission to include a plurality of paths, each corresponding to a different one of a plurality of keys used for one of encrypting and decrypting data streams. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide system and method for decoupling encryption of one plain text block from the encryption of the next plain text block and encryption apparatus can be placed in parallel to increase throughput through the encryption circuit as suggested by Markham in (column 3: lines 35-40; column 4: lines 4-8).

As per claim 13:

Admission discloses a parallel stream operation apparatus, wherein the input stream processing unit converts the plurality of data streams to a format that is useable as content data before outputting each data stream to the one of the paths that corresponds to a key that, from among the plurality of keys, is for one of encrypting and decrypting the data stream (figure 1: 1621 stream processing unit).

As per claim 14:

Admission discloses a parallel stream operation apparatus, wherein the input stream processing unit converts the plurality of data streams to a packetized elementary stream packet format before outputting each data stream to the one of the paths that corresponds to a key that-, from among the plurality of keys, is for one of encrypting and decrypting the data stream (0010).

7. Claims 8-9 and 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Admitted prior art by applicant (hereinafter referred to as Admission) in view of Markham (US Pat. No.: 5, 796, 836) and further in view of Goff et al. (hereinafter referred to as Goff, US Pat. No.: 6,347,143).

As per claim 8:

Admission and Markham do not explicitly disclose an input stream processing unit multiplexes at least two of the plurality of data streams to generate one data stream. Goff, in

analogous art, however, discloses an input stream processing unit multiplexes at least two of the plurality of data streams to generate one data stream (figure 2: 55-58). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Admission and Markham to include an input stream processing unit multiplexes at least two of the plurality of data streams to generate one data stream. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide additional protection against attacks on secrecy cryptographic device which includes a de-multiplexer, a plurality of encryption blocks, a plurality of permutation blocks, and a multiplexer as suggested by Goff in (column 1: lines 60-67; column 2: lines 15-20).

As per claim 9:

Goff discloses a parallel stream operation apparatus, wherein the input stream processing unit de-multiplexes one of the input data streams to generate a plurality of data streams (figure 1: intelligent de-multiplexer).

As per claim 16:

Admission discloses a television reception apparatus wherein the data streams include at least video data and audio data (0006).

As per claim 17:

Goff discloses an input stream processing unit multiplexes at least two of the plurality of data streams to generate one data stream (figure 2: 55-58).

As per claim 18:

Goff discloses an input stream processing unit demultiplexes one of the input data streams to generate a plurality of data streams (figure 2: 51-53).

As per claim 19:

Admission discloses an input stream processing unit converts the plurality of data streams to a packetized elementary stream packet format before outputting each data stream to the one of the paths that corresponds to a key that, from among the plurality of keys, is for one of encrypting and decrypting the data stream (0006; 0010).

Allowable Subject Matter

8. Claims 3-6 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

9. The following is a statement of reasons for the indication of allowable subject matter: In a parallel stream operation a simplified and an improved throughput of encryption and decryption of the stream data is required. A simplified and less complicated operation is provided for selection a key in the operation step each time stream data in input. Particularly in

TV reception, applying this program to a parallel stream operation that has a plurality of paths that correspond respectively to a plurality of keys for encryption and/or decryption, complicated operations for selecting a key each time stream data is input are avoided.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See the notice of reference cited in form PTO-892 for additional prior art

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is (571) 273-3784. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T-G

Techane Gergiso

Patent Examiner

Art Unit 2137

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

May 13, 2007